Spring 2017 Cryptography and Network Security

Homework 2

Release Date: 4/12/2017

Due Date: 5/3/2017, 23:59

Instruction

- **Submission Guide:** Please submit all your codes and report to CEIBA. You need to put all of them in a folder named by your student id, compress it to hw1_{student_id}.zip. For example, hw1_r04922456.zip.
- You may encounter new concepts that haven't been taught in class, and thus you're encouraged to discuss with your classmates, search online, ask TAs, etc. However, you must write your own answer and code. Violation of this policy leads to serious consequence.
- You may need to write some programs in the Capture The Flag (CTF) problems. Since you can use any programming language you like, we will use a pseudo extension code**.ext** (e.g., code.py, code.c) when referring to the file name in the problem descriptions.
- You are recommended to provide a brief usage of your code in **readme.txt** (e.g., how to compile, if needed, and execute). You may lose points if TAs can't run your code.
- In each of the Capture The Flag (CTF) problems, you need to find out a flag, which is in `BALSN{...}` format, to prove that you have succeeded in solving the problem.
- Besides the flag, you also need to submit the code you used and a short write-up in the report to get full points.
- In some CTF problems, you need to connect to a given service to get the flag. These services only allow connections from 140.112.0.0/16 and 140.118.0.0/16.

Handwriting

1. Encryption Algorithms (10%)

Give two differences between symmetric and asymmetric cryptography, and give two examples for each method. To achieve higher security, which method usually needs a larger key? Which method is generally faster, why?

2. Three-way Diffie-Hellman (10%)

We've discussed the techniques to establish a shared key between two individuals using Diffie-Hellman key agreement in class. Now, can we modify the protocol to establish a key shared by three individuals A, B, and C? Assuming the public values, *prime* and *generator*, are p , g respectively. We also assume that the attacker is passive, meaning that the attacker can eavesdrop, but not modify, the message being sent between the individuals. The total number of steps that **send messages** from one individual to another shouldn't be more than **6**, and only one-to-one communication is allowed. The fewer steps your protocol takes, the higher score you will gain. However, you get zero point if the adversary (i.e., the TAs) can break your protocol.

3. ElGamal threshold decryption (15%)

In this problem, we want you to combine ElGamal public-key encryption and Shamir's secret sharing.
First, let's recall the ElGamal encryption scheme.
`setup:`

$$\begin{aligned} \text{large prime} &: p \\ \text{generator} &: g \\ \text{secret key} &: sk_B = b \\ \text{public key} &: pk_B = g^b (\text{mod } p) \end{aligned}$$

`encryption:`

$$\begin{aligned} \text{plaintext} &: m \\ \text{random value} &: x \\ \text{ciphertext1} &: c_1 = g^x (\text{mod } p) \\ \text{ciphertext1} &: c_2 = m(pk_b)^x (\text{mod } p) \end{aligned}$$

`decryption:`

$$\text{plaintext} : m = c_2 c_1^{-b} (\text{mod } p)$$

Now you should revise the setting above to accomplish ElGamal threshold decryption, such that the ciphertext can be decrypted only if t out of n users collaborate.

Hint: Genarally, you only need to change the section of setup and the section of decryption.

Capture The Flag

4. ECB Encryption Mode (10%)

We talk about modes of operation when introducing block ciphers. A mode of operation describes how to repeatedly apply a cipher's single-block operation securely to transform data larger than a block. One of the encryption modes is the Electronic Codebook (ECB) mode. ECB mode is simple, but vulnerable. Therefore, in this homework, you are going to break a login service `ECB_Encryption_Mode/login.py` by exploiting ECB mode vulneralbility. You can access the service by `nc 140.112.31.109 10004`. Try to get the flag behind the service and explain how you solve the problem in your write-up. Save you script (if exists) as `code4.ext`.

Hint: Do you know the cut-and-paste-attack?

5. Beginner's RSA (20%)

(1) (4%) Hi, My name is Tom. I am a secret agent. If you want to be a secret agent like me, you have to pass the training. Here is a RSA public key and an encrypted flag. I won't give you the private key. Can you decrypt the flag?

(2) (8%) Both you and Alice received RSA keys from a trusted (but lazy) central authority. Your public key is in `RSA2/pubkey` and your private key is in `RSA2/prikey`. Now you have observed the public key of Alice (in `RSA2/Alice_pubkey`) and an encrypted message (in `RSA2/cipher`), can you tell what the secret is?

(3) (8%) Since you leaked the secret of Alice in (2), you have been kicked out from the communication group. This time, you observe the public keys and the ciphers of Alice and Bob (in `RSA3/Alice` and `RSA3/Bob` respectively). You know that they encrypted the same message. Can you tell what the message is without d?

6. Digital Certificate (5%)

Hello, I am Tom's friend, Wombat, a secret agent, too. My mission is to investigate a secret organization. In order to obtain valuable information, we have to pass a certificate checking service to impersonate a member of the organization. Luckily, I had just heard that if we want to pass the checking service, we can fake a X.509 certificate `fake.crt` with following `issuer` information, encode the whole text of the certificate (include the 'BEGIN' and 'END' tag) in `base64` format and send it to the checking service.

```
Country = TW
Locality = R307
Organization = BALSN
Organization Unit = Security
```

```
Common Name = www.balsn.com
Email Address = cns@balsn.com
```

Your certificate should look like:

```
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

You can access the checking service by `nc 140.112.31.109 10005`. Besides, part of the checking service is provided in `Digital_Certificate/check_cert.py`. Try to get the valuable information and flag, and explain how you pass the certificate checking service in your write-up.

7. I need your help (10%)

It's me, Tom. I believe you have pass the training. It's time for a real mission. Last week, I stole a big secret from bad people. Since it's a secret, it is encrypted by a public key. You will receive the encrypted secret and private key. However, the private key was redacted by them. Can you recover it? The whole world is counting on you. Please explain how you recover the private key.

8. I will look for you, and I will find you (20% + 10%)

The flag of the following challenges is `BALSN{Server IP}` except the first one.

(1) (2%) Connect to `ab6qqnuetobsjslu.onion:31337` to get the flag.

(2) (3%) Find the IP of `https://ab6qqnuetobsjslu.onion:10443`.
Hint: Is the self-signed certificate really necessary?

(3) (7%) Find the IP of `ztczadd4tipwhwyl.onion:22`.
Hint: Let me Shodan that for you.

(4) (8%) Find the IP of `7zysy3slgt7qxhek.onion:21`.
Hint: Make sure you use the latest `torsocks` or set the `tordns_deadpool_range` to `127.42.42.0/255.255.255.0`.

(5) (10%) **Bonus:** Find the IP of `su7twnwqamobiytx.onion:31337`. Try
`cat <(echo Knock, knock) - | torify ncat su7twnwqamobiytx.onion 31337`